CLAIMS

What is claimed is:

1. An apparatus comprising:

a plurality of modular exponentiators including a first modular exponentiator and a second modular exponentiator; and

a coupling device interposed between said first modular exponentiator and said second modular exponentiator to receive a control signal and to selectively couple said first modular exponentiator to said second modular exponentiator in response to a state of said control signal.

2. The apparatus as set forth in claim 1, said apparatus having a first mode of operation corresponding to a first state of said control signal wherein said first modular exponentiator is operably separated from said second modular exponentiator and a second mode of operation corresponding to a second state of said control signal wherein said first modular exponentiator is operably coupled to said second modular exponentiator via said coupling device.

3. The apparatus as set forth in claim 2, wherein said first modular exponentiator and said second modular exponentiator operate as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit modular exponentiator in said second mode of operation, where n is an integer.

4. The apparatus as set forth in claim 3, wherein n equals 512.

5. The apparatus as set forth in claim 1, wherein each of said plurality of modular exponentiators comprises a modular multiplier to perform a modular multiplication of the form A x B mod M, where A, B, and M are all integers.

6. The apparatus as set forth in claim 5, wherein said modular multiplier comprises a Montgomery multiplier.

7. The apparatus as set forth in claim 5, wherein said modular multiplier comprises a systolic array of processing elements.

8. The apparatus as set forth in claim 1, wherein said a coupling device comprises a multiplexer.

9. An apparatus comprising:

a plurality of modular multipliers including a first modular multiplier and a second modular multiplier;

a coupling device interposed between said first modular multiplier and said second modular multiplier to receive a control signal and to selectively couple said first modular multiplier to said second modular multiplier in response to a state of said control signal.

10. The apparatus as set forth in claim 9, said apparatus having a first mode of operation corresponding to a first state of said control signal wherein said first modular multiplier is operably separated from said second modular multiplier and a second mode of operation corresponding to a second state of said control signal wherein said first modular multiplier is operably coupled to said second modular multiplier via said coupling device.

11. The apparatus as set forth in claim 10, wherein said first modular multiplier and said second modular multiplier operate as two n-bit modular multipliers in said first mode of operation and as a single 2n-bit modular multiplier in said second mode of operation, where n is an integer.

12. The apparatus as set forth in claim 11, wherein n equals 512.

13. The apparatus as set forth in claim 9, wherein each of said plurality of modular multipliers comprises a Montgomery multiplier.

14. The apparatus as set forth in claim 9, wherein each of said plurality of modular multipliers comprises a systolic array of processing elements.

15. The apparatus as set forth in claim 9, wherein said a coupling device comprises a multiplexer.

16. A processor comprising:

a plurality of modular exponentiators including a first modular exponentiator and a second modular exponentiator; and

a coupling device interposed between said first modular exponentiator and said second modular exponentiator to receive a control signal and to selectively couple said first modular exponentiator to said second modular exponentiator in response to a state of said control signal.

17. The processor as set forth in claim 16, said processor having a first mode of operation corresponding to a first state of said control signal wherein said first modular exponentiator is operably separated from said second modular exponentiator and a second mode of operation corresponding to a second state of said control signal wherein said first modular exponentiator is operably coupled to said second modular exponentiator via said coupling device.

18. The processor as set forth in claim 17, wherein said first modular exponentiator and said second modular exponentiator operate as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit modular exponentiator in said second mode of operation, where n is an integer.

19. The processor as set forth in claim 18, wherein n equals 512.

20. The processor as set forth in claim 16, wherein said a coupling device comprises a multiplexer.

21. A system comprising:

a memory to store data and instructions;

a first processor coupled to said memory to process data and execute instructions; and

a second processor coupled to said memory, said second processor comprising:

a plurality of modular exponentiators including a first modular exponentiator and a second modular exponentiator; and

a coupling device interposed between said first modular exponentiator and said second modular exponentiator to receive a control signal and to selectively couple said first modular exponentiator to said second modular exponentiator in response to a state of said control signal.

22. The system as set forth in claim 21, said second processor having a first mode of operation corresponding to a first state of said control signal wherein said first modular exponentiator is operably separated from said second modular exponentiator and a second mode of operation corresponding to a second state of said control signal wherein said first modular exponentiator is operably coupled to said second modular exponentiator via said coupling device.

23. The system as set forth in claim 22, wherein said first modular exponentiator and said second modular exponentiator operate as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit modular exponentiator in said second mode of operation, where n is an integer.

24. A method comprising:

receiving a control signal;

selectively coupling a first modular exponentiator to a second modular exponentiator of a plurality of modular exponentiators in response to a state of said control signal;

receiving a plurality of operands; and

performing a modular exponentiation operation on said plurality of operands utilizing said first modular exponentiator and said second modular exponentiator.

25. The method as set forth in claim 24, wherein selectively coupling a first modular exponentiator to a second modular exponentiator of a plurality of modular exponentiators in response to a state of said control signal comprises:

operably separating said first modular exponentiator from said second modular exponentiator in a first mode of operation corresponding to a first state of said control signal; and

operably coupling said first modular exponentiator to said second modular exponentiator in a second mode of operation corresponding to a second state of said control signal.

26. The method as set forth in claim 25, wherein performing a modular exponentiation operation on said plurality of operands utilizing said first modular exponentiator and said second modular exponentiator comprises:

operating said first modular exponentiator and said second modular exponentiator as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit modular exponentiator in said second mode of operation, where n is an integer.

27. A machine-readable medium having a plurality of machine-executable instructions embodied therein which when executed by a machine, cause said machine to perform a method comprising:

receiving a control signal;

selectively coupling a first modular exponentiator to a second modular exponentiator of a plurality of modular exponentiators in response to a state of said control signal;

receiving a plurality of operands; and

performing a modular exponentiation operation on said plurality of operands utilizing said first modular exponentiator and said second modular exponentiator.

28. The machine-readable medium as set forth in claim 27, wherein selectively coupling a first modular exponentiator to a second modular exponentiator of a plurality of modular exponentiators in response to a state of said control signal comprises:

operably separating said first modular exponentiator from said second modular exponentiator in a first mode of operation corresponding to a first state of said control signal; and

operably coupling said first modular exponentiator to said second modular exponentiator in a second mode of operation corresponding to a second state of said control signal.

29. The machine-readable medium as set forth in claim 28, wherein performing a modular exponentiation operation on said plurality of operands utilizing said first modular exponentiator and said second modular exponentiator comprises:

operating said first modular exponentiator and said second modular exponentiator as two n-bit modular exponentiators in said first mode of operation and as a single 2n-bit modular exponentiator in said second mode of operation, where n is an integer.